"ROLE OF TECHNOLOGY IN IDENTIFYING CYBER CRIMES IN INDIA – A STUDY"

Synopsis Submitted to

Swami Ramanand Teerth Marathwada University Nanded

For the Award of the Degree of

Doctor of Philosophy (Ph.D.)

In Law

Under the Faculty of Humanities

Under the Guidance of

Dr. Waseem Ullah Khan
(LL.M., Ph.D., NET, JRF, DCL)
Assistant Professor,
Shivaji Law College, Parbhani

By
Shital Shamrao Adkine
2023

1. Introduction:

The world economy has shifted its paradigm from manufacturing to service-driven to all-inclusive economy since last two decades. There were major revolutionary reforms which took place in several parts of globe influencing the national economies. International geo-political conditions (BREXIT), warlike circumstances (Russia-Ukraine), international marketplaces, COVID-19 pandemic, government reforms are some of the major factors responsible for the changing scenario in different countries. India plays a key role in Asia-Pacific region. It has been playing a pivotal role in establishing the peace and order in not only Asia but also other continents. It gives the first priority to develop healthy relations with neighbouring countries. At the same time, internal as well as external security, protection of highly confidential data of national security agencies, strategic plans, safeguarding the interests of citizens are equally important for any government. India, being a developed economy, needs to plan and execute various strategies from safety and security perspectives. The term 'Cybercrime' refers to criminal activities that are committed using computers, networks, or the internet. With the rapid advancement of technology and increased connectivity, cybercrime has become a significant global concern.[1]

2. Scope and Significance of Study:

Internet has shown tremendous growth in the world and India respectively. According to Statista Report, there were 5.16 Billion internet users in the world in April, 2023. Out of the total, 4.76 Billion (59.4%) are the social media users. It shows the rise in the number of internet users.

However, it is also found that the social media and other online portals become the hotspot for online frauds, identity thefts and terrorist networking in the digital era. Thousands of citizens becoming the victims of cyber crimes in different parts of country. They have been facing financial losses, threat for their own identities, data theft. Unfortunately, there are very few cyber police stations available in India in proportion to population.[5] In addition, the victims also hesitate to register complaints of cyber crime due to lack of awareness or willingness. The present study aims to understand the factors responsible for the rising number of cyber crimes and less awareness towards the same. The Government of India introduced Information Technology Act 2000. However, it has not been reached to last person staying in the rural, women, senior citizens of country. Addressing the issue of cyber crime can minimize the increasing burden legislative bodies and safeguard the interests of digital citizens in India. India has witnessed a significant rise in financial cybercrimes,

---

[1]Bernik, I. Cybercrime. Cybercrime and Cyberwarfare, (2014), 1- 56. Available at: https://doi.org/10.1002/9781118898604.ch1

[5]Crime Bureau Investigation (CBI). www.cbi.nic.in

including credit card fraud, online banking fraud, and identity theft. These crimes often involve phishing attacks, where individuals are deceived into revealing their financial details. Indian companies have faced several high-profile data breaches, resulting in the compromise of sensitive information of millions of individuals. These incidents highlight the need for stronger cybersecurity measures to protect data. With the increased adoption of social media platforms in India, instances of cyberbullying, online harassment, and spreading fake news have risen. Such activities can have severe consequences on the mental well-being of individuals.[6]

3. Objectives of Study:

The proposed research has following objectives:

1. To study the concept of cybercrime
2. To examine the major types of cyber-crimes in Chhatrapati Sambhajinagar district
3. To know the awareness level of cybercrimes amongst the digital citizens in Chhatrapati Sambhajinagar district
4. To understand the major challenges faced by digital citizens in Chhatrapati Sambhajinagar district
5. To analyze effectiveness of IT Act 2000 in prevention of cybercrimes in Chhatrapati Sambhajinagar district
6. To suggest better solutions to overcome the challenges and minimize the cybercrimes in Chhatrapati Sambhajinagar district

4. Statement of the Problem:

Cyber crime has become a grave concern for corporations, governments, organizations, individuals, security agencies and multi-national companies across the globe. It has different forms and purposes. Cyber attacks on confidential data may question the existence or growth of an organization at times.[7] With the rapid advancement of technology and increased connectivity, cybercrime has become a significant global concern. Malware and Ransomware Attacks, Phishing, Identity Theft, Data Breaches, Online Scams and Fraud and Cyberbullying are some of the most visible forms of cyber crimes in the world.[8]

---

[6]National Crime Bureau Board. "Crime in India- 2018." NCRB, (Jan 28, 2021), https://ncrb.gov.in/crime-india-2018

[7]Kabay, M. E. "Studies and Surveys of Computer Crime." *Focus,* (2000). Available at: http://securityportal.com/cover/coverstory2001211.html

[8]Seamus O Clardhuanin. "An Extended Model of Cybercrime Investigations." *International Journal of Digital Evidence*, (Summer 2004), Vol. 3, Issue 1

Malicious software is developed to penetrate computer systems and networks, including spyware, worms, viruses, and Trojan horses, among others. A form of virus known as ransomware encrypts user data and requests payment in order to decrypt it. Phishing is the practice of convincing someone to divulge private information, like login credentials or financial information, by appearing as a reliable organisation through emails, texts, or phoney websites.[9] To commit fraud or engage in other illegal activity, cybercriminals take personal data such as social security numbers, credit card information, or bank account details. Data breaches happen when hackers access private data without authorization, exposing important details like customer information or business secrets. Numerous online frauds prey on unwary people to steal their money or personal information, including lottery, expenditure, and love frauds. The use of technology, especially social media sites, email, or messaging services, to bully, menace, or intimidate someone online.[10]

5. Review of Literature:

Md. Abu Bakar Siddik, & Saida Talukder Rahi. (2021) studied examine the overall scenario of cyber crime and various initiatives taken by the Government in Bangladesh. It is found that the number of internet users have increased drastically in the last 5 years. The social media networking sites such as Facebook has given birth to cyber crimes in Bangladesh in particular. The Government enacted Bangladesh Telecommunication Regulation Act in 2001. However, it did not succeed in overcoming the challenges of cyber crimes in Bangladesh. As a result, Digital Security Act and ICT Act were introduced in the year 2018 to combat the changing nature and forms of cyber crimes.[11]

The Information Technology Bill was approved by the Indian Parliament's two chambers in May 2000. The Information Technology Act of 2000 was created after the President gave his assent to the bill in August 2000. The IT Act of 2000 contains cyberlaws. The purpose of this Act is to set up the legal framework for online shopping in India. Additionally, the cyber regulations significantly affect India's emerging economy and online businesses. Therefore, it's critical to comprehend the IT Act of 2000's many views and what it has to offer.

---

[9]Etter B. "The challenges of Policing Cyberspace." Presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand. (2002).

[10]Etter, B. "The forensic challenges of E-Crime." Current Commentary No. 3 *Australasian Centre for Policing Research, Adelaide*. (2001).

[11]Md. Abu Bakar Siddik, & Saida Talukder Rahi. (2021). Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context. BiLD Law Journal, 5(1), 68–92. Retrieved from https://bildbd.com/index.php/blj/article/view/34

The Information Technology Act of 2000 also intends to establish the legal framework necessary to give all electronic records and other actions conducted via electronic means legal sanctity. According to the Act, an agreement of acceptance may, unless otherwise agreed, be expressed using electronic means of communication and shall have full legal validity and effect.[12]

Cyber Morphing has become popular method of cyber crime in India. It is a type of crime wherein the original image is edited by unauthorized user to possess a fake identity. Generally, the female photos are used on such fake accounts. Pornographic messages, videos are posted to attract youngsters. It is punishable act under Section 43 and 66 of Information Act 2000.[13] One of the biggest difficulties facing Indian and international law enforcement in the future is cybercrime, or criminal activity on the Internet. As ICT spreads even more, elements of electronic crime will be present in all types of criminal activity, including those that are today seen as more traditional. It already plays a role in numerous international crimes involving the trafficking of illegal drugs, trafficking of persons, terrorist activities, and money laundering. We must be ready to handle this new issue as electronic proof becomes more prevalent, even in traditional crimes. To assure safety and security on the Internet, law enforcement agencies from all around the world are collaborating to create new alliances, new forensic techniques, and new strategies for combating cybercrime. To identify, stop, combat, and react to cybercrime, new methods of investigation, technological advances, and abilities will need to be used in a global environment. New types of crime, a considerably wider scope and scale of being victimised, the need to respond much more quickly, and difficult technical and legal complications will all be the features of this "new business." To resolve the severe jurisdictional concerns, creative solutions like the establishment of "cybercops," "cybercourts," and "cyberjudges" may someday be necessary.[14] Even though hacking may be considered illegal in some nations, information security professionals who are knowledgeable about hacking are needed to combat cyberthreats in the areas of business, politics, social media, and national security. Wall (2007)[15] makes the claim that foreign criminals steal intellectual property for their own benefit or at their governments' orders.

---

[12]MeitY- Government of India- cybercrime.gov.in

[13] Phillips, Kirsty, et al. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic Sciences* 2.2 (2022): 379-398

[14]Singh, H. P., and Tareq S. Alshammari. "An institutional theory perspective on developing a cyber security legal framework: a case of saudi arabia." Beijing L. Rev. 11 (2020): 637.

[15]Wall, D. "Cybercrime: The transformation of crime in the Information Age." Polity, (2007).

An annual loss of $10 billion is predicted. For instance, Germany assessed its own IP losses from industrial espionage at $25 to $50 billion, with a large portion of these losses being brought on by lax internet security. Notably, the majority of businesses fail to report damage caused by cybercrimes, suggesting that the actual number may be greater. In order to prevent frightening investors and consumers, other companies that have been hacked decide to keep the information secret. Cybercriminals have been increasingly focusing on the financial sector. They frequently target payment cards, accounts with online banks, and ATM machines.[16]

Another common way of cyber crime is Email Spoofing. Though it is known, it's challenging to trace the sender of an email. Most often, email spoofing is used to illegally get personal information and private photographs from women, which are then used to blackmail them. A research claims that since 2016, incidents of phishing have increased by 280%. According to Avanan research, around 4% of the emails that a person receives are fake emails. Section 66-D of the Information Technology Amendment Act of 2008 and Sections 417, 419, and 465 of the Indian Panel Code of 1860 both make email spoofing a crime. With the consent of the court where investigation of the offence is underway, it is a considered cognizable admissible for bail and compounded offence that may be tried by any magistrate.[17]

Cybercrime is punishable under numerous statutes and regulations. However, the Indian Penal Code (IPC), 1860, and the Information Technology Act (IT Act), 2000, are the sources of almost all of the regulations. The IPC is India's general penal code, which outlines transgressions and stipulates penalties for them. IPC, which has been legally updated and judiciously considered to be enforceable against cybercriminals, comprises laws and punishments relating to the real world. The IT Act, on the other hand, is a particular code that addresses the use of information technology and crimes that are committed using it. The IT Amendment Act, which includes several cybercrimes, was passed in 2008. In terms of cybercrime against women, the IT Act and IPC work in tandem.[18]

---

[16]Jain, Nilesh and Shrivastav Vibhash. "Cyber Crime Changing Everything – An Empirical Study." International Journal of Computer Application, Issue 4, Volume 1 (February 2014). Available at: https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY

[17]Grispos, G. "Criminals: Cybercriminals." *Encyclopedia of Security and Emergency Management*, (2019), 1- 7. Available at: https://doi.org/10.1007/978-3-319-69891-5_80-1

[18]Jain, Nilesh and Shrivastav Vibhash. "Cyber Crime Changing Everything – An Empirical Study." International Journal of Computer Application, Issue 4, Volume 1 (February 2014). Available at: https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY

Victims of cybercrime in India face several challenges that can significantly impact their ability to seek justice and recover from the consequences of the crime. Many individuals in India are unaware of the various forms of cybercrime, their rights as victims, and the available legal remedies. This lack of awareness often leads to underreporting of cybercrimes and delays in seeking appropriate assistance. Victims may face difficulties in reporting cybercrimes due to complex reporting procedures, lack of user-friendly reporting mechanisms, or limited accessibility to law enforcement agencies. The process of reporting cybercrimes may involve multiple agencies, and victims may struggle to navigate through the bureaucracy.

Cybercrimes often involve perpetrators located in different geographic locations, which can create challenges in determining jurisdiction and initiating legal action. Cooperation and coordination between different law enforcement agencies, both within India and internationally, are essential. Insufficient investment in cybersecurity technologies, tools, and personnel can hinder the prevention, detection, and response to cyber threats.[19] There are certain limitations found in the existing acts in India. The criminal involved in cyber crime might use their smart and creative brains to find the gap and take undue advantages at times.[20]. The IPC's Sections 499 and 507 have not been invoked in response to generalized sexist remarks. Furthermore, doxing that doesn't involve the exchange of explicit material or harassment is excluded. The act of doxing by hacking is not specifically mentioned in Section 66 of the IT Act, which criminalises hacking. Sections 499 and 507 of the IPC and Section 66 of the IT Act treat online harassment, verbal abuse, and hacking for doxing as private, isolated crimes. Violence that results in physical harm, as opposed to interference with bodily integrity and private freedom of choice, as defined by the other provisions of the IT Act and IPC, is an exception under Section 66E of the IT Act and provisions 354C and 354D of the Criminal Laws Amendment Act of 2013. Additionally, those sections only address "physical privacy" rather than "informational privacy."[21] Samuel McQuade[22] in his book described that cyber crime had been increasing like a slow poison.

---

[19]India Forensic Report. "Case of Cyber Extortion." India Forensic, (Jan 20, 2021), Available at: http://www.indiaforensic.com/cyberextortion.htm

[20]Rani, Sita, et al. "Threats and corrective measures for IoT security with observance of cybercrime: A survey." *Wireless Communications and Mobile Computing* 2021 (2021): 1-30.Available at: https://downloads.hindawi.com/journals/wcmc/2021/5579148.pdf

[21]Lallie, Harjinder Singh, et al. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & security* 105 (2021): 102248.Available at: https://www.sciencedirect.com/science/article/pii/S0167404821000729

[22]McQuade, Samuel C. *Understanding and managing cybercrime*. Boston: Pearson/Allyn and Bacon, 2006.

The techno-savvy and experts are involved targeting the soft corners such as college students, women, senior citizens. The emails and text messages were used for establishing the network with the devices. The governments and concerned authorities did pay much attention to address the concern. It was a challenge for developed economies. However, developing and underdeveloped economies had a long way to understand the hidden impact of cyber crimes on individuals, women and economy by and large.

Another book by Broadhurst and Grabosky[23] (2005) discussed how cyber crime in Asian continent has been deeply rooted and spreading through the youths. The concern was so serious that it established direct and indirect linkages with the terrorist activities in Asia. The countries like India had to pay huge price thereafter. The major challenge was raising the awareness, detecting the cyber crimes, and investigating them. The Information Technology Act was passed in India. However, it took several years to implement it successfully.

The edited copy of book Martellozzo and Emma[24] comments about the victims of cyber crimes. By the year 2017, there was sound awareness regarding the social media. Slowly and steadily the social networking sites were launched attracting millions of youths, entertaining them and creating networks. Unknown friend request, spam messages, unauthorized calls, pop-up and micro scanners became the tools for spying the users. The new social media users became the victims of the same. Though some acts were introduced, very few times implementation was visible. Many times, the cases were not registered due to lack of willingness by the complainant as well as policies authorities.

Grabosky[25] in his book made an attempt to view criminology from the lenses of judicial mechanisms. It is observed that there different perspectives and mechanisms proposed and practiced in different countries of the world. In fact, controversies are found when it comes to tackling the growing concern of cyber crimes. This may be due to intensification, types of users and different forms of cyber crimes, diversified communities etc. The various experts noted minute observations regarding the meticulous planning and time-bound, result-oriented outcomes to deal with it. A book by Gillespie[26] makes us familiar with the various issues and critical challenges emerged after the cyber crimes.

---

[23]Broadhurst, Rod, and Peter Grabosky. *Cyber-crime: The challenge in Asia*. Vol. 1. Hong Kong University Press, 2005.

[24]Martellozzo, Elena, and Emma A. Jane, eds. *Cybercrime and its victims*. Taylor & Francis, 2017.

[25]Grabosky, Peter. *Keynotes in criminology and criminal justice series: Cybercrime*. Oxford University Press, 2016.

[26]Gillespie, Alisdair A. *Cybercrime: Key issues and debates*. Routledge, 2019.

There was unexpected and sudden surge in the use of social media in 2019. The reason responsible for the same was COVID-19 pandemic outbreak. It made people compulsory to sit at home. Some worked from home while many were sitting idle due to loss of jobs, and government restrictions imposed. Since social media was used more, many cases were observed in various countries. There were financial fraud more as compared to other. Cyber attacks for information of important firms, sensitive data hacking were noticed from time to time. Fake accounts creation was more during this time.

The authors named Halder, Debarati, and K. Jaishankar[27] (2016) dealt with the cyber-crime from a different perspective. They studied and discussed about the cybercrime against the women in particular. Another salient feature of the book is Indian context. India is a country of young people. Millions of youths have active users of various social networking apps. It is found that the women were soft targets for the cyber attackers. Many times, they didn't dare to express due to fear of failure and mental stress. More awareness camps need to be scheduled in schools, colleges.

Sundaram and Syed[28] (2011) in their edited book critically examined how cyber crime disrupted the social as well as digital disorder. Due to the advanced and high-end technologies, various online platforms, tools have been integrated for the ease and comfort. However, it created long-lasting digital disorders for the users indirectly. The social media apps were converted into payment platforms creating financial crimes, psychological stress, fake identities etc. The syncing facilities wherein accessing the multiple apps/platforms through same profiles created multiple opportunities for the hackers.

Sesha Kethineni illustrated the recent scenario of cyber crimes in India from legal perspective. The Information Technology Act 2000 and its effectiveness, challenges in implementation, regulations made by the law and enforcement mechanisms are the major points of discussions in the book. It is praiseworthy to note that some universities have introduced cyber security as a value addition course for the undergraduate and post-graduate students educating them on cyber security. The online courses are offered at minimize prices to some extent.

---

[27]Halder, Debarati, and K. Jaishankar. *Cyber crimes against women in India*. SAGE Publications India, 2016.

[28]Sundaram, P. Madhava Soma, and Syed Umarhathab, eds. *Cyber crime and digital disorder*. K. Jaishankar, 2011

6. Research Methodology:

The research methodology is the blueprint of study. It gives clarity about the overall future plan of research to be carried out in a step by step manner.

Table 1: Proposed Research Model of Study

Sr. No.	Description	Details
1]	Research Type	Hybrid (Quantitative)
2]	Research Method	Survey Method
3]	Sampling Method	Simple Random Sampling Method
4]	Population of Study	100- UG/PG Students 100- Working Professionals 100- Women
5]	Sample Size	300
6]	Target Respondents	Gender: Male and Female from Chhatrapati Sambhajinagar district (All 7 Tehsils)
7]	Data Type	Primary & Secondary
8]	Primary Data Collection Instrument	Online/ Offline Questionnaire

*Sample size is tentative figure.

- **Data Type: Primary and Secondary Data**

The collection of data from valid, verifiable sources is an integral part of the research study. All ethical considerations are also taken into account by the researcher during the study. Both primary and secondary data is used in this research based on the objectives set for the study.

- **Primary Data:** Online/Offline Survey of Target Respondents

- **Secondary Data:** It consists of various industry reports, research journals and articles, case studies, government reports, official websites, magazines, newspapers articles, blogs, expert opinions and some other authentic sources are parts of secondary data for the research study. It is ensured that the sources are competent and authoritative from validity point of view.

7. Hypotheses of Study:

Hypothesis 1:

Social Media causes harm to citizens in Chhatrapati Sambhajinagar district.

Hypothesis 2:

There is no association between education and cyber crimes victimization in Chhatrapati Sambhajinagar district.

Hypothesis 3:

There is no association between social media and cyber crimes in Chhatrapati Sambhajinagar district.

Hypothesis 4:

The Information Technology Act is not effective to safeguard interests, privacy of women in Chhatrapati Sambhajinagar district.

8. Limitations of Study:

The present study has the following limitations:

- It is restricted to the subject discipline of information technology and law in particular.
- The Indian laws and legal contexts are taken into consideration
- It is applicable to the geographical area of Chhatrapati Sambhajinagar district in Maharashtra State in particular.

9. Chapter Scheme:

The proposed study consists of total seven chapters as below:

CHAPTER I: Introduction

CHAPTER II: Cyber Crime: Trends, Practices and Legal Implications

CHAPTER III: Judicial Approach to Cyber Crime in India

CHAPTER IV: Cyber Crime: Challenges and Implications

CHAPTER V: Cyber Crime and IT Act 2000

CHAPTER VI: Data Analysis & Interpretation

CHAPTER VII: Conclusion and Suggestions

Conclusion and Suggestions:

All of the above discussion shows that technology has both pros and cons for individuals, societies, governments and economies to the great extent. Internet is the gift for users connecting the world. It offers many more advantages such as work from home, online shopping, documentations, sharing instant message, online transactions, entertainment etc. However, it has equal risks and threats from hackers, cyber attackers in the forms of viruses leaking personal, professional, company details. Along with the internet users, cyber crimes have also been increased in proportion. Social media is the soft target in this regard. India is a developing economy. It has several initiatives to monitor, control cyber crimes including Information Technology Act 2000. However, taking the changing nature, forms and dimensions of cyber crimes into account, it needs more deep level and strict provisions. In addition, people should be trained, guided on know-how of cyber crimes to raise the awareness and protect all of them.

References/Bibliography

[1]Bernik, I., Cybercrime. Cybercrime and Cyberwarfare, (2014), 1- 56. Available at: https://doi.org/10.1002/9781118898604.ch1

[2]KPMG. "E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation, USA. (2000).

[3]International crime and Cyber Terrorism. Available at: http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp

[4]The Ministry of Electronics and IT, Government of India. (6th June, 2022). "Putting the Interests of Digital Indians First." Available at: https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf

[5]Crime Bureau Investigation (CBI). www.cbi.nic.in

[6]National Crime Bureau Board. "Crime in India- 2018." NCRB, (Jan 28, 2021), https://ncrb.gov.in/crime-india-2018

[7]Kabay, M. E. "Studies and Surveys of Computer Crime." *Focus*, (2000). Available at: http://securityportal.com/cover/coverstory2001211.html

[8]Seamus O Clardhuanin. "An Extended Model of Cybercrime Investigations." *International Journal of Digital Evidence,* (Summer 2004), Vol. 3, Issue 1

[9]Etter B. "The challenges of Policing Cyberspace." Presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand. (2002).

[10]Etter, B. "The forensic challenges of E-Crime." Current Commentary No. 3 *Australasian Centre for Policing Research, Adelaide*. (2001).

[11]Md. Abu Bakar Siddik, & Saida Talukder Rahi. (2021). Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context. BiLD Law Journal, 5(1), 68–92. Retrieved from https://bildbd.com/index.php/blj/article/view/34

[12]MeitY- Government of India- cybercrime.gov.in

[13] Phillips, Kirsty, et al. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic Sciences* 2.2 (2022): 379-398

[14]Singh, H. P., and Tareq S. Alshammari. "An institutional theory perspective on developing a cyber security legal framework: a case of saudi arabia." Beijing L. Rev. 11 (2020): 637.

[15]Wall, D. "Cybercrime: The transformation of crime in the Information Age." Polity, (2007).

[16]Jain, Nilesh and Shrivastav Vibhash. "Cyber Crime Changing Everything – An Empirical Study." International Journal of Computer Application, Issue 4, Volume 1 (February 2014). Available at: https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY

[17]Grispos, G. "Criminals: Cybercriminals." *Encyclopedia of Security and Emergency Management*, (2019), 1- 7. Available at: https://doi.org/10.1007/978-3-319-69891-5_80-1

[18]Jain, Nilesh and Shrivastav Vibhash. "Cyber Crime Changing Everything – An Empirical Study." International Journal of Computer Application, Issue 4, Volume 1 (February 2014). Available at: https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY

[19]India Forensic Report. "Case of Cyber Extortion." India Forensic, (Jan 20, 2021), Available at: http://www.indiaforensic.com/cyberextortion.htm

[20]Rani, Sita, et al. "Threats and corrective measures for IoT security with observance of cybercrime: A survey." *Wireless Communications and Mobile Computing* 2021 (2021): 1-30.Available at: https://downloads.hindawi.com/journals/wcmc/2021/5579148.pdf

[21]Lallie, Harjinder Singh, et al. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & security* 105 (2021): 102248.Available at: https://www.sciencedirect.com/science/article/pii/S0167404821000729

[22]McQuade, Samuel C. *Understanding and managing cybercrime*. Boston: Pearson/Allyn and Bacon, 2006.

[23]Broadhurst, Rod, and Peter Grabosky. *Cyber-crime: The challenge in Asia*. Vol. 1. Hong Kong University Press, 2005.

[24]Martellozzo, Elena, and Emma A. Jane, eds. *Cybercrime and its victims*. Taylor & Francis, 2017.

[25]Grabosky, Peter. *Keynotes in criminology and criminal justice series: Cybercrime*. Oxford University Press, 2016.

[26]Gillespie, Alisdair A. *Cybercrime: Key issues and debates*. Routledge, 2019.

[27]Halder, Debarati, and K. Jaishankar. *Cyber crimes against women in India*. SAGE Publications India, 2016.

[28]Sundaram, P. Madhava Soma, and Syed Umarhathab, eds. *Cyber crime and digital disorder*. K. Jaishankar, 2011.

Research Student

Shital Shamrao Adkine

Research Supervisor

Dr. Waseem Ullah Khan
(LL.M, Ph.D, NET, JRF, DCL)
Assistant Professor,
Shri. Shivaji Law College, Parbhani.